# Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath, Gilles Peskine

2025-06-16

# Recent community activity (thank you!)

- tls#10219 awesomekosm - Added shallow clone for submodules
- tls#10200 aslze - [3.6] Fix build C++ apps with MSVC
- tls#10112 etienne-lms - [Backport 3.6] Fix build warning related to deprecated DTLS connect ID
- tls#10202 LoveKarlsson - [3.6] Fix alignment problems with IAR and Zephyr
- tls#10113 etienne-lms - Fix build warning related to deprecated DTLS connect ID
- tls#8933 Biswa96 - pkg-config: fix static linking in Windows
- crypto#258 ccrugoPhilips - Fix MSVC build issue from MbedTls issue 7087
- crypto#216 DemiMarie - asn1parse: Require minimal-length encodings of lengths
- crypto#152 LoveKarlsson - Fix IAR alignment issues if __packed has been redefined into a macro.
- crypto#262 irwir - Add winsock2 header into build_info.h
- crypto#301 ilie-halip-nxp - scripts: driver_templates: call driver init/free

# Recent community activity (thank you!)

## Valerio @Nordic

- tls#10213 valeriosetti - [development] PK: try storing all private RSA keys in PSA (2/3)
- tls#10187 valeriosetti - [development] Always enable MBEDTLS_PK_USE_PSA_EC_DATA + use PSA interruptible operations as backend for PK restartable ones
- tls#10041 valeriosetti - [development] Make mbedtls_psa_register_se_key usable with opaque drivers
- tls#9371 valeriosetti - psasim: use shared memory as messaging system for client-server communication
- tls#9400 valeriosetti - PSA client-server: test parity report
- merged: tls#10192 valeriosetti - [development] Some pre-requisites for psa#299
- frame#171 valeriosetti - [framework] PK: try storing all private RSA keys in PSA (1/3)
- frame#145 valeriosetti - [framework] Make mbedtls_psa_register_se_key usable with opaque drivers
- frame#166 valeriosetti - [framework] Always enable MBEDTLS_PK_USE_PSA_EC_DATA
- frame#170 valeriosetti - [framework] PK: try storing all private RSA keys in PSA
- merged: frame#154 valeriosetti - [framework] Add components-compiler.sh
- crypto#308 valeriosetti - [tf-psa-crypto] PK: try storing all private RSA keys in PSA (3/3)
- crypto#191 valeriosetti - [tf-psa-crypto] Make mbedtls_psa_register_se_key usable with opaque drivers
- merged: crypto#299 valeriosetti - [tf-psa-crypto] Always enable MBEDTLS_PK_USE_PSA_EC_DATA + use PSA interruptible operations as backend for PK restartable ones
- crypto#306 valeriosetti - [tf-psa-crypto] PK: try storing all private RSA keys in PSA
- merged: crypto#248 valeriosetti - [tf-psa-crypto] Add components-compiler.sh

# Major activities within core team

https://github.com/orgs/Mbed-TLS/projects/18

- TF-PSA-Crypto
  - First standalone components are now running in the CI
- Mbed TLS 4.0/TF-PSA-Crypto 1.0
  - Last stages of MVP investigation
  - Making low level crypto functions internal
  - Removing legacy types from public non-PSA interfaces
  - Defining release process for split repositories

# Release Timeline

- 1.0/4.0 currently aiming for September 2025
- 3.6 LTS supported until early 2027
  - 3.6.1 (Aug 2024): mostly fixes related to TLS 1.3
  - 3.6.2 (Oct 2024): security fix
  - 3.6.3 (March 2024): supports a PSA key store in builds without malloc
  - 3.6.4 (planned 30 June 2024): GCC 15 support, other bug and security fixes

arm

Thank You
Danke
Gracias
Grazie
谢谢
ありがとう
Asante
Merci
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה
ధన్యవాదములు